REMARKS

Status of Claims:

By way of the instant amendment, claims 2, 4, 6 and 8 have been cancelled. Claims 9 and 10 have been added. Thus, claims 1, 3, 5 and 7 and 9-10 remain for examination.

Acknowledgement of Priority Document:

The examiner is requested to acknowledge the filing and receipt of the certified copy of applicant's priority document filed together with applicant's claim for priority with the originally filed application on March 23, 2003.

Prior Art Rejections:

Claims 1-8 stand rejected under 35 USC 103 as unpatentable over Fiammante in view of Gile.

The examiner's rejection is respectfully traversed.

Fiammante is directed toward a secure commercial transaction apparatus and method in which both a PC and a mobile terminal are required to complete the transaction. The PC is used because of its large display and friendly user interface whereas the mobile telephone is used for its built-in security features inherent to wireless mobile devices (see Par. [0008]). The PC is used to initiate the business transaction, but ultimately the mobile telephone is needed to provide the pirvate key or smart card to effectively "sign" for the commercial transaction. As stated in par [0022] in reference to Fiammante Fig. 4:

> User 100 approves the commercial transaction when user 100 is satisfied with the contents and the objects of the transaction. Upon receipt of the approval, business application 210 uses table 300 to identify an identification record of user 100. Upon identifying an identification record of user 100, servlet 220 contacts mobile phone 140 through network 135, a gateway 175, and a tower 170 via communication link 190, a communication link 191, a communication link 192, and communication link 165. Servlet 220 then sends a signature request to mobile phone 140 according to the Wireless

> Application Protocol (WAP). User 100 uses a private key of smart card 155 to sign for the commercial transaction. Business application 210 and servlet 220 complete the transaction upon receipt of the signature of user 100. Those having ordinary skill in the art will appreciate that the commercial transaction meets all the goals of confidentiality, authentication, integrity and non-repudiation.

Fiammante is not concerned with purchase AND authentication of a purchaser of tickets, nor is he concerned with the particular problems to which applicant's invention is directed. As stated in the background section of applicant specification, the traditional use of a bar code on a mobile telephone to purchase tickets if fraught with problems especially the fact that a third part other than the true purchaser may use the tickets. The ticket buyer may, for example, sell the ticket to a third party at an exorbitant price or a third party may illegally use a stolen ticket.

In order to address these problems applicant's invention used biological information, such as one or more fingerprints to insure that the person who bought the ticket is the SAME PERSON that is standing at the entrance to the ticketed event and attempting to user the electronic ticket to enter the ticketed event. Thus, the authentication terminal 40 is used at the entrance to the ticketed event, and the mobile terminal is used to input to the authentication terminal both the identity of the mobile user (e.g., the telephone number of the mobile user) and the biological information previously downloaded to the mobile unit from the ticket issuing center. This biological information is termed "first" biological information in the language of applicant's claims. Additionally, the purchaser of the ticket must input in present time, his/her own biological information into the authentication unit at the time authentication is required (e.g., just before entering the area where the ticketed event is to take place). This inputted biological information is termed the "second" biological information in the language of the claims. The authentication unit then compares the first and second biological information to determine if the person who bought the ticket originally (using the mobile terminal in communication with the ticket issuing center) is the same person who is presently standing in front of the authentication unit entering his/her biological information (e.g., fingerprint). This authentication ensures that the purchaser of the ticket is not selling

the ticket to another person (third party) and further insures that a third party who perhaps found or stole the ticket, is not using the ticket to gain entry into the ticketed event.

In the language of applicant's claim 1, there is recited:

> 1. (Currently Amended) An electronic ticket issuing system, comprising:
>
> a mobile terminal including a storage for storing an electronic ticket;
>
> a ticket issuing center;
>
> an authentication department; and
>
> an authentication terminal, wherein:
>
> the mobile terminal, the ticket issuing center, the authentication department, and the authentication terminal are connected to each other via a network, and the authentication terminal is connected to the mobile terminal to perform authentication between a ticket buyer and an electronic ticket;
>
> first biological information which indicates unique physical characteristics of the ticket buyer is registered in advance in the authentication department;
>
> the mobile terminal transmits a request for ticket purchase to the ticket issuing center;
>
> the ticket issuing center transmits a request for issue of an electronic certificate to the authentication department to request the authentication department to issue an electronic certificate which corresponds to the request for ticket purchase transmitted from the mobile terminal and which validates the ticket buyer;
>
> the authentication department creates an electronic certificate including the pre-registered first biological information on the basis of the request for issue of an electronic certificate transmitted from the ticket issuing center, and transmits the electronic certificate to the ticket issuing center;
>
> the ticket issuing center creates an electronic ticket to which the electronic certificate transmitted from the authentication department is added, and transmits the electronic ticket to the mobile terminal;

the mobile terminal stores the electronic ticket transmitted from the ticket issuing center in the storage; and

wherein:

at the time of authentication:

(1) the mobile terminal transmits the electronic ticket stored in the storage to the authentication terminal;

(2) second biological information which indicates unique physical characteristics of the ticket buyer is input into the authentication terminal; and

(3) the authentication terminal performs authentication by comparing the first biological information, which is contained within the electronic certificate added to the electronic ticket, with the second biological information, and outputs a corresponding authentication result.

The underlined portions of the above claim 1 emphasize the differences between applicant's invention and the applied prior art Fiammante and Gile references. Fiammante does not utilize biological information as apparently recognized by the examiner. Gile uses fingerprint data to determine which students who are suppose to attend a class are not actually present. Thus Gile compares the fingerprints of those students entering a class with a class roster and by the process of elimination, determines which students did not enter the class. Both Fiammante and Gile are completely silent as to the problems addressed by applicant's invention and thus, not surprising, are silent about the particular solution adopted and claimed by applicant.

In order to expedite prosecution of the application, applicant has combined the recitations of original claim 2 into claim 1 and has further combined the recitations of claim 6 into claim 5. Further new claim 9 (similar to apparatus claim 1) and claim 10 (similar to method claim 5) have been added. These claims are all deeded to clearly define the invention over the prior art and to be patentable thereover. None of the prior art uses the first and second biological information in the manner recited in applicant's claims. As such the PTO has not made out a *prima facie* case of obviousness within the provisions of 35 USC 103.

Conclusions:

Applicant believes that the present application is now in condition for allowance. Favorable reconsideration of the application as amended is respectfully requested.

The Examiner is invited to contact the undersigned by telephone if it is felt that a telephone interview would advance the prosecution of the present application.

The Commissioner is hereby authorized to charge any additional fees which may be required regarding this application under 37 C.F.R. §§ 1.16-1.17, or credit any overpayment, to Deposit Account No. 19-0741. Should no proper payment be enclosed herewith, as by a check being in the wrong amount, unsigned, post-dated, otherwise improper or informal or even entirely missing, the Commissioner is authorized to charge the unpaid amount to Deposit Account No. 19-0741. If any extensions of time are needed for timely acceptance of papers submitted herewith, Applicant hereby petitions for such extension under 37 C.F.R. §1.136 and authorizes payment of any such extensions fees to Deposit Account No. 19-0741.

Respectfully submitted,

Date January 6, 2005

By 

FOLEY & LARDNER LLP
Customer Number: 22428
Telephone: (202) 672-5407
Facsimile: (202) 672-5399

David A. Blumenthal
Attorney for Applicant
Registration No. 26,257